Available online at www.sciencedirect.com

ScienceDirect

Finite Fields and Their Applications 14 (2008) 258–276

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Syntactical and automatic properties of sets of polynomials over finite fields

Michel Rigo

Institute of Mathematics, University of Liège, Grande Traverse 12 (B37), B-4000 Liège, Belgium

Received 13 July 2006; revised 5 May 2007

Available online 27 June 2007

Communicated by D. Panario

Abstract

Syntactical properties of representations of integers in various number systems are well known and have been extensively studied. In this paper, we transpose the notion of recognizable set of integers into the framework of the polynomial ring over a finite field $\mathbb{F}$. We define B-recognizable sets of polynomials over $\mathbb{F}$ and consider their first properties.

Keywords: Recognizable set; Automata; Numeration system; Polynomial over a finite field

1. Introduction

All along this paper $\mathbb{F}$ is a finite field of prime characteristic p containing $q = p^t$ elements, $t \geqslant 1$. Let $\mathbb{F}[X]$ be the polynomial ring over $\mathbb{F}$. This polynomial ring shares a lot of properties with $\mathbb{Z}$: it is a principal ideal domain, every residue class ring modulo a nonzero ideal has finitely many elements, it is a Euclidian domain and also a unique factorization domain. In particular, the strong analogy between $\mathbb{Z}$ and $\mathbb{F}[X]$ has been extensively studied in number theory [1,8]. Here we consider the point of view of number systems and study the first (and quite easy) related syntactical properties.

E-mail address: m.rigo@ulg.ac.be.

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2007.06.002

If $P \in \mathbb{F}[X]$ we denote its degree by $\deg(P)$ and we assume that the degree of the zero polynomial is $-\infty$. The set of polynomials over $\mathbb{F}$ of degree less than n is denoted by $\mathbb{F}[X]_{<n}$. Any positive integer n can be decomposed using an integer base $k > 1$ as

$$n = \sum_{i=0}^{\ell} c_i k^{\ell-i}, \quad c_0 \neq 0,$$

and the uniqueness of this decomposition follows from the fact that all the integer coefficients c_i are less than k [10]. In the same way, if B is a polynomial of degree $b > 0$, then any polynomial P can be decomposed as

$$P = \sum_{i=0}^{\ell} C_i B^{\ell-i}, \quad C_0 \neq 0, \tag{1}$$

the decomposition being unique provided that the polynomials C_i belong to $\mathbb{F}[X]_{<b}$.

Notice for instance that this framework of number system over $\mathbb{F}[X]$ was recently used to study the distribution of the corresponding additive functions [7]. Moreover, the two classical concepts of canonical number systems and β-numeration systems, $\beta > 1$ being real, have also been generalized to polynomial rings over finite fields [12,16,17]. In the latter case, β is then a formal Laurent series over $\mathbb{F}$ used to develop elements of the field of formal Laurent series. Notice also that our considerations are a special case of automatic maps on semirings with digits developed in [2].

This paper should be quite easy to follow for reader used to k-ary expansions and is organized as follows. In Section 2, we define the concept of B-recognizability of a subset of $\mathbb{F}[X]$ (for a reference on recognizability in the integer case see [5] or [13, Chapter 7]) and we introduce a subsequent concept of recognizable sets of integers mixing k-ary expansions and polynomial expansions. In Section 3, we show that adding two B-recognizable sets gives again a B-recognizable set and that multiplication by a fixed polynomial also preserves B-recognizability. In Section 4, we restrict the general concepts of automatic map and kernel [2] to the framework of polynomials over a finite field. Section 5 deals with the problem of the dependence of the recognizability of a subset of $\mathbb{F}[X]$ with respect to the choice of the polynomial playing the role of the base. Section 6 is independent, we discuss the sequentiality of the multiplication and Euclidian division within $\mathbb{F}[X]$. In what follows, we assume the reader familiar with automata theory (see for instance [9] for details).

Since many of the results presented in this paper are easy adaptations of the classical setting, let us briefly mention which of our results have no counterpart in the usual k-ary case: Remark 3 leads to a "strange" concept of recognizability and we exhibit nonstandard examples of sets of integers recognizable in that sense (like the set of numbers obtained from Pascal's triangle mod 2 converted to decimal), Proposition 8 considers multiplication of the base by a constant, Remark 6 gives the flavour of what could be Cobham's theorem in this setting. Let us also mention Example 10 and Proposition 13 where evaluation of polynomials is considered.

In what follows, the finite field $\mathbb{F}$ containing $q = p^t$ and a polynomial $B \in \mathbb{F}[X]$ of degree $b > 0$ are given once and for all.

2. Numbering of $\mathbb{F}[X]$

Using a standard greedy algorithm any nonzero polynomial P can be uniquely written as (1). Let k be the unique integer such that

$$kb \leqslant \deg(P) < (k+1)b.$$

Set $R_0 := P$ and consider the Euclidian division of R_0 by B^k,

$$R_0 = C_0 B^k + R_1 \quad \text{with } \deg(R_1) < kb.$$

Next consider the successive Euclidian divisions of $R_1, R_2, \ldots, R_{k-1}$ by $B^{k-1}, B^{k-2}, \ldots, B$ respectively to obtain $C_1, \ldots, C_{k-1}$, R_k and set $C_k := R_k$.

Remark 1. One can obtain first the polynomial C_k by considering the Euclidian division of P by B, i.e., $Q_0 := P = Q_1 B + C_k$ with $\deg(C_k) < b$. Next, divide Q_1 by B to obtain $Q_1 = Q_2 B + C_{k-1}$. Successive Euclidian divisions of $Q_2, \ldots, Q_k$ by B provide $C_{k-2}, \ldots, C_0$.

Let $P = f_0 X^n + \cdots + f_n$ be a polynomial in $\mathbb{F}[X]_{<b}$, we define a function $\Phi : \mathbb{F}[X]_{<b} \to \mathbb{F}^b$ by

$$\Phi(P) := (\underbrace{0, \ldots, 0}_{b-n-1}, f_0, \ldots, f_n)$$

and this definition naturally extends to the zero polynomial. Notice that Φ is a trivial isomorphism between the two $\mathbb{F}$-vector spaces $\mathbb{F}[X]_{<b}$ and $\mathbb{F}^b$.

Definition 1. Any nonzero polynomial P can be uniquely decomposed as in (1), $P = \sum_{i=0}^{k} C_i B^{k-i}$ and we say that the word

$$\rho_B(P) = \Phi(C_0)\Phi(C_1)\ldots\Phi(C_{k-1})\Phi(C_k)$$

over the finite alphabet $\mathbb{F}^b$ is the *B-representation* of P. By convention, the representation of the polynomial zero is the empty word ε.

Example 1. Let $\mathbb{F} = \mathbb{Z}/3\mathbb{Z}$ (with elements denoted by $0, 1, 2$) and the polynomials $B = X^2 + 2X + 2$ and $P = X^8 + 2X^7 + X^5 + 2X^4 + 2X^3 + X + 2$ over $\mathbb{F}$. Applying successive Euclidian divisions, we get

$$P = 1 \cdot B^4 + 1 \cdot B^3 + (2X + 2) \cdot B^2 + (2X + 1) \cdot B + 1$$

and therefore, the B-representation of P is the word of length 5 over $(\mathbb{Z}/3\mathbb{Z})^2$,

$$\rho_B(P) = (0, 1)(0, 1)(2, 2)(2, 1)(0, 1).$$

Remark 2. A B-representation never begins with the element $(0, \ldots, 0) =: \mathbf{0}$. Consequently, the function ρ_B is a one-to-one correspondence between $\mathbb{F}[X]$ and $\{\varepsilon\} \cup (\mathbb{F}^b \setminus \{\mathbf{0}\})(\mathbb{F}^b)^*$. We shall denote its reciprocal map by π_B. Moreover, we allow π_B to be defined on words beginning with $\mathbf{0}$'s: we set $\pi_B(\mathbf{0}^n u) = \pi_B(u)$.

The central notion of B-recognizable subset of $\mathbb{F}[X]$ is defined as follows.

Definition 2. A set $\mathcal{T} \subseteq \mathbb{F}[X]$ is said to be *B-recognizable* if the language

$$\rho_B(\mathcal{T}) = \{\rho_B(P) \mid P \in \mathcal{T}\} \subseteq (\mathbb{F}^b)^*$$

is regular (i.e., accepted by a finite automaton). As a consequence of the previous remark, a set $\mathcal{T} \subset \mathbb{F}[X]$ is B-recognizable if and only if $\mathbf{0}^*\rho_B(\mathcal{T})$ is regular. Therefore, if we deal simultaneously with several representations of various length (for instance when considering the operation of addition), it is often easier to admit leading **0**'s in the B-representations to obtain words of the same length.

Remark 3. Any nonnegative integer n can be written in base q as

$$n = c_0 q^\ell + \cdots + c_\ell \quad \text{with } 0 \leqslant c_i < q.$$

We can define a one-to-one correspondence μ between $\mathbb{N}$ and the polynomial ring $\mathbb{F}[X]$ induced by a one-to-one correspondence between $\{0, \ldots, q-1\}$ and $\mathbb{F}$ (since it does not lead to any confusion, we use the same notation for the two mappings). Indeed, assume that to each coefficient $c \in \{0, \ldots, q-1\}$ in the above decomposition corresponds a given element $\mu(c)$ in $\mathbb{F}$. (We assume furthermore that $\mu(0)$ is the zero element in $\mathbb{F}$.) Therefore, to n corresponds the polynomial

$$\mu(n) := \mu(c_0)X^\ell + \cdots + \mu(c_\ell).$$

The number of such one-to-one mappings μ between $\{0, \ldots, q-1\}$ and $\mathbb{F}$ (and also the number of the induced one-to-one mappings between $\mathbb{N}$ and $\mathbb{F}[X]$) is $(q-1)!$.

As an example, consider once again $q = 3$ and $\mathbb{F} = \mathbb{Z}/3\mathbb{Z}$. The integer 11 is decomposed as $11 = 1 \cdot 3^2 + 0 \cdot 3 + 2$. We associate the polynomial $\mu(11) = X^2 + 2$ over $\mathbb{F}$ (we have chosen μ to map each integer coefficient 0, 1, 2 onto its corresponding residue class also denoted 0, 1, 2).

Notice that μ is not a monoid morphism between $\mathbb{N}$ and $\mathbb{F}[X]$. Indeed, $23 = 2 \cdot 3^2 + 1 \cdot 3 + 2$ and $11 + 23 = 34 = 1 \cdot 3^3 + 0 \cdot 3^2 + 2 \cdot 3 + 1$. But

$$\mu(34) = X^3 + 2X + 1 \neq \mu(11) + \mu(23) = X + 1.$$

This latter remark is independent of the mapping μ between $\{0, \ldots, q-1\}$ and $\mathbb{F}$. (The reason will be obvious in the next section where the question of carry is discussed: for addition within $\mathbb{N}$ a carry can propagate to the left but not in the case of $\mathbb{F}[X]$ where $\deg(P+Q) \leqslant \sup\{\deg(P), \deg(Q)\}$.)

Thanks to the latter discussion, we can introduce a new kind of recognizable set of integers.

Definition 3. Let B be a polynomial of degree $b > 0$ over the field $\mathbb{F}$ with q elements and μ be a one-to-one correspondence between $\{0, \ldots, q-1\}$ and $\mathbb{F}$ (where $\mu(0) = 0$). We say that a subset $\mathcal{T} \subseteq \mathbb{N}$ of nonnegative integers is *(q, μ, B)-recognizable* if $\rho_B(\mu(\mathcal{T}))$ is a regular language over $(\mathbb{F}^b)^*$.

This notion seems at first rather artificial, but some well-known sequences can be shown as (q, μ, B)-recognizable. Notice that these examples are strongly related to the so-called "linear cellular automata induced by a Laurent polynomial" [3].

Example 2. Consider the set $\mathcal{T}$ of numbers obtained from Pascal's triangle mod 2 converted to decimal (Sloane's sequence A001317 [18]):

$$\left\{ t_n = \sum_{j=0}^{n} \left(\binom{n}{j} \bmod 2 \right) 2^j \;\middle|\; n \geqslant 0 \right\}$$
$$= \{1, 3, 5, 15, 17, 51, 85, 255, 257, 771, 1285, 3855, 4369, 13107, 21845, 65535, 65537, \ldots\}.$$

Let us take $q = 2$, $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$, $B = 1 + X$ and $\mu : \{0, 1\} \to \mathbb{F}$ mapping each integer coefficient 0, 1 in base two onto its corresponding residue class also denoted 0, 1. With such choices, it is obvious that $\mathcal{T}$ is $(2, \mu, 1 + X)$-recognizable. Over $\mathbb{Z}/2\mathbb{Z}$, we have

$$\mu(t_n) = \sum_{j=0}^{n} \left(\binom{n}{j} \bmod 2 \right) X^j = (1 + X)^n$$

and we get $\rho_B(\mu(\mathcal{T})) = 1\,0^*$. On the other hand, it is not difficult to see that for $n \in \mathbb{N}$,

$$\left[\forall i = 0, \ldots, n\colon \binom{n}{i} \equiv 1 \pmod 2 \right] \quad \Leftrightarrow \quad \exists k \geqslant 0\colon\ n = 2^k - 1.$$

Therefore, if the set $\mathcal{T}$ was 2-recognizable, i.e., if the set $\mathcal{T}_2$ of binary expansions of elements in $\mathcal{T}$ was a regular language over $\{0, 1\}$, then

$$\mathcal{T}_2 \cap 1^* = \left\{ (1)^{2^k} \;\middle|\; k \geqslant 0 \right\}$$

would be regular (notice that $t_{2^k-1} = 2^{2^k} - 1$). But using a classical pumping argument, we get a contradiction. Notice that it also means that $\mu(\mathcal{T}) \subseteq \mathbb{F}[X]$ is $(1 + X)$-recognizable but not X-recognizable. (Observe that $\mathcal{T}$ is 2-recognizable if and only if $\mu(\mathcal{T})$ is X-recognizable.)

Example 3. Consider the set $\mathcal{S}$ of numbers $\mathcal{S} = \{s_n \mid n \geqslant 0\}$ (Sloane's sequence A038184 [18]) such that s_n is the nth line generated by an elementary cellular automaton using "Rule 150":

000	001	010	011	100	101	110	111
0	1	1	0	1	0	0	1

and starting from $s_0 = 1$ [19] and interpreted as a binary number,

$$\mathcal{S} = \{1, 7, 21, 107, 273, 1911, 5189, 28123, 65793, 460551, 1381653, 7039851, \ldots\}.$$

This generating process works as follows. Take a line $\ldots 00100 \ldots$ (where for convenience an arbitrary number of zeroes, at least 2, has been put on both sides of $s_0 = 1$) and consider a window of size 3 sliding over this line (just like for sliding block codes used in symbolic dynamics). Rules like this "Rule 150" define a mapping from the set $\{0, 1\}^3$ of possible factors seen through the

window of size 3 to $\{0, 1\}$, for instance: $010 \mapsto 1$. Applying this sliding window map on the line, we obtain the second line as $\ldots 0011100 \ldots$ and we forget the extra zeroes to get $s_1 = 111$, i.e., the binary representation of 7. This process is repeated with this latter line and so on.

In the same way, the previous example could have been obtained using "Rule 60":

000	001	010	011	100	101	110	111
0	0	1	1	1	1	0	0

With the same setting as in the previous example, but considering $B = 1 + X + X^2$, we get for all $n \geqslant 0$,

$$\mu(s_n) = \left(1 + X + X^2\right)^n.$$

Indeed, "Rule 150" just reflects how multiplication by $1 + X + X^2$ is performed. Thus $\mathcal{S}$ is $(2, \mu, 1 + X + X^2)$-recognizable.

One can play the same game with other polynomials of degree 2, $B = X^2 + 1$ corresponds to the set of integers (Sloane's sequence `A038183`)

$$\{1, 5, 17, 85, 257, 1285, 4369, 21845, 65537, 327685, 1114129, 5570645, \ldots\}$$

generated with "Rule 90"

000	001	010	011	100	101	110	111
0	1	0	1	1	0	1	0

and $B = X^2 + X$ to the set (Sloane's sequence `A117998`)

$$\{1, 6, 20, 120, 272, 1632, 5440, 32640, 65792, 394752, 1315840, 7895040, \ldots\}$$

generated with "Rule 102"

000	001	010	011	100	101	110	111
0	1	1	0	0	1	1	0

Example 4. The *modulo M inverse binomial transform* of a sequence $(a_n)_{n\geqslant 0}$ is a sequence $(b_n)_{n\geqslant 0}$ given by

$$\forall n \geqslant 0, \quad b_n := \sum_{k=0}^{n} \left(\binom{n}{k} \bmod M \right) a_k.$$

The modulo 2 inverse binomial transform of $(8^n)_{n\geqslant 0}$ (Sloane's sequence `A100311`) starts with

$$1, 9, 65, 585, 4097, 36873, 266305, 2396745, 16777217, 150994953, \ldots$$

The corresponding set of numbers is $(2, \mu, 1 + X^3)$-recognizable but not 8-recognizable (and thus not 2-recognizable thanks to Cobham's theorem [6]). Indeed, this is just the generalization of Example 2. For $k \geqslant 1$, let

$$\mathcal{T}^{(k)} = \left\{ t_n^{(k)} = \sum_{j=0}^{n} \left(\binom{n}{j} \bmod 2 \right) (2^k)^j \;\middle|\; n \geqslant 0 \right\}.$$

Therefore, considering numbers written in base 2 and working over $\mathbb{Z}/2\mathbb{Z}$,

$$\mu\big[t_n^{(k)}\big] = \sum_{j=0}^{n} \left(\binom{n}{j} \bmod 2 \right) X^{kj} = \big(1 + X^k\big)^n$$

and we can conclude in the same way as in Example 2.

3. Arithmetic operations

For integer base systems, performing the addition of two integers usually leads to the apparition of a carry. The situation in $\mathbb{F}[X]$ is easier. Let P, Q be two polynomials such that

$$P = C_0 B^k + \cdots + C_k \quad \text{and} \quad Q = D_0 B^k + \cdots + D_k,$$

where, in the above decomposition, at least C_0 or D_0 is nonzero but one of the two can be zero if $|\lfloor \frac{\deg(P)}{b} \rfloor - \lfloor \frac{\deg(Q)}{b} \rfloor| > 0$. Obviously, we have the following unique decomposition of their sum:

$$P + Q = (C_0 + D_0) B^k + \cdots + (C_k + D_k),$$

where $C_i + D_i$ is the sum of two polynomials of $\mathbb{F}[X]$ of degree less than b and is again a polynomial of degree less than b. Otherwise stated, no carry occurs for the addition in $\mathbb{F}[X]$,

$$\rho_B(P + Q) = \Phi(C_0 + D_0) \cdots \Phi(C_k + D_k) = \big(\Phi(C_0) + \Phi(D_0)\big) \cdots \big(\Phi(C_k) + \Phi(D_k)\big).$$

In the above formula, we have assumed that $C_0 + D_0 \neq 0$. Otherwise, the B-representation of $P + Q$ has to start with the first nonzero polynomial $C_i + D_i$.

Proposition 1. *Let B be a polynomial of degree $b > 0$ over $\mathbb{F}$. If $\mathcal{S}, \mathcal{T}$ are two B-recognizable subsets of $\mathbb{F}[X]$, then $\mathcal{S} + \mathcal{T}$ is also B-recognizable.*

Proof. We can easily build a single state automaton (the unique state is initial and final) reading 3-tuples of letters in $\mathbb{F}^b$ and recognizing the regular language

$$L := \left\{ \begin{pmatrix} u \\ v \\ w \end{pmatrix} : u, v, w \in \big(\mathbb{F}^b\big)^*,\ |u| = |v| = |w|,\ \pi_B(u) + \pi_B(v) = \pi_B(w) \right\}.$$

The loops of this automaton are labeled by 3-tuples of letters in $\mathbb{F}^b$

$$\begin{pmatrix} (f_0,\ldots,f_{b-1}) \\ (g_0,\ldots,g_{b-1}) \\ (f_0+g_0,\ldots,f_{b-1}+g_{b-1}) \end{pmatrix},$$

where $f_i, g_i \in \mathbb{F}$ and the addition $f_i + g_i$ is considered within $\mathbb{F}$. Consider the canonical morphisms $p_j : (\mathbb{F}^b)^3 \to \mathbb{F}^b$, $j = 1, 2, 3$, defined by

$$p_j \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = x_j.$$

It is clear that $p_1^{-1}[\mathbf{0}^*\rho_B(\mathcal{S})]$ and $p_2^{-1}[\mathbf{0}^*\rho_B(\mathcal{T})]$ are regular (the set of regular languages is closed under morphisms and inverse morphisms). To conclude the proof, observe that

$$p_3\big(p_1^{-1}\big[\mathbf{0}^*\rho_B(\mathcal{S})\big] \cap p_2^{-1}\big[\mathbf{0}^*\rho_B(\mathcal{T})\big] \cap L\big)$$

is a regular language. □

As a consequence of this result, translation by a fixed polynomial preserves the B-recognizability of a set.

Corollary 2. *Let B be a polynomial of degree $b > 0$ over $\mathbb{F}$. If $\mathcal{S}$ is a B-recognizable subset of $\mathbb{F}[X]$, then $\mathcal{S} + \{P\}$ is also B-recognizable, for any $P \in \mathbb{F}[X]$.*

Proof. It is a direct consequence of the previous proposition since $\{\rho_B(P)\}$ is a finite language which is thus regular. □

Multiplication of a subset of $\mathbb{F}[X]$ by a fixed polynomial also preserves B-recognizability.

Proposition 3. *Let B, Q be two polynomials with $\deg(B) \geqslant 1$. If $\mathcal{T} \subseteq \mathbb{F}[X]$ is B-recognizable then $Q.\mathcal{T}$ is also B-recognizable.*

Proof. The case $\deg(Q) = 0$ is immediate. Multiplication of $P = \sum_{i=0}^{k} C_i B^{k-i}$ by a nonzero constant γ belonging to $\mathbb{F}$ induces a permutation $\nu : \Phi(C_i) \mapsto \Phi(\gamma.C_i)$ of the elements in $\mathbb{F}^b$ between $\rho_B(P)$ and $\rho_B(\gamma.P)$, since $\gamma.P = \sum_{i=0}^{k}(\gamma.C_i)B^{k-i}$. In what follows, we assume therefore that $\deg(Q) > 0$.

Let P be an arbitrary polynomial in $\mathbb{F}[X]$ of the form $P = C_0B^k + \cdots + C_k$ with $C_0 \neq 0$ and $\deg(C_i) < b$. If Q is such that $\deg(Q) = n > 0$ then

$$P.Q = \sum_{i=0}^{k}(C_i.Q)B^{k-i} \quad \text{with } \deg(C_i.Q) \leqslant n + b - 1.$$

We can write $n + b - 1$ as $\beta b + r$ with $\beta \in \mathbb{N} \setminus \{0\}$ and $0 \leqslant r < b$. For each $C_i \in \mathbb{F}[X]_{<b}$, we can write

$$C_i.Q = D_{i,0}B^{\beta} + \cdots + D_{i,\beta} \quad \text{with } \deg(D_{i,j}) < b,\ \forall j \in \{0,\ldots,\beta\}, \tag{2}$$

and the polynomials $D_{i,j}$ are uniquely determined by C_i, Q and B. Our aim is to build an automaton $\mathcal{A}$ reading pairs of letters in $\mathbb{F}^b$ and accepting the reversal of the language

$$L := \left\{ \begin{pmatrix} u \\ v \end{pmatrix} : \exists u, v \in \left(\mathbb{F}^b\right)^*,\ |u| = |v|,\ Q.\pi_B(u) = \pi_B(v) \right\}.$$

The set of states of $\mathcal{A}$ is $(\mathbb{F}^b)^\beta$, the initial state is $(0,\dots,0)$ and it is also the unique final state. For each C_i satisfying a relation of the form (2) (there are q^b such polynomials C_i) we have an edge from state $(r_{\beta-1},\dots,r_0)$ with label

$$\begin{pmatrix} \Phi(C_i) \\ r_{\beta-1} + \Phi(D_{i,\beta}) \end{pmatrix}$$

to the state

$$\big(r_{\beta-2} + \Phi(D_{i,\beta-1}),\dots, r_0 + \Phi(D_{i,1}), \Phi(D_{i,0})\big),$$

additions being interpreted in the $\mathbb{F}$-vector space $\mathbb{F}^b$. This comes simply from the fact that

$$P.Q = \sum_{i=0}^{k} \sum_{j=0}^{\beta} D_{i,j} B^{\beta+k-i-j}.$$

Using canonical morphisms of projection, one can conclude with the same reasoning as in the proof of Proposition 1. (The reader has also to remember that the set of regular languages is closed under reversal.) □

Example 5. In this short example, we present the construction introduced in the previous proof. We use the same notation. Consider once again the polynomial $B = X^2 + 2X + 2$ over $\mathbb{F} = \mathbb{Z}/3\mathbb{Z}$ and the polynomial $Q = X^2 + 1$. Hence, $b = n = 2$ and $\beta = 1$. Table 1 list all polynomials of degree less than 2 and their decomposition after multiplication by Q in the polynomial base B. This table will be useful to define the automaton $\mathcal{A}$. Take the polynomial $P = X^8 + 2X^7 + X^5 + 2X^4 + 2X^3 + X + 2$ over $\mathbb{F}$ such that $\rho_B(P) = (0,1)(0,1)(2,2)(2,1)(0,1)$. One can check that

$$\rho_B(P.Q) = (0,1)(1,0)(0,0)(1,0)(1,2)(1,2).$$

Table 1
$\Phi(C_i.Q) = \Phi(D_{i,0})\Phi(D_{i,1})$, i.e., $C_i.Q = D_{i,0}B + D_{i,1}$

i	$\Phi(C_i)$	$C_i.Q$	$D_{i,0}$	$\Phi(D_{i,0})$	$D_{i,1}$	$\Phi(D_{i,1})$
1	$(0,0)$	0	0	$(0,0)$	0	$(0,0)$
2	$(0,1)$	X^2+1	1	$(0,1)$	$X+2$	$(1,2)$
3	$(0,2)$	$2X^2+2$	2	$(0,2)$	$2X+1$	$(2,1)$
4	$(1,0)$	X^3+X	$X+1$	$(1,1)$	1	$(0,1)$
5	$(1,1)$	X^3+X^2+X+1	$X+2$	$(1,2)$	X	$(1,0)$
6	$(2,1)$	X^3+2X^2+X+2	X	$(1,0)$	$2X+2$	$(2,2)$
7	$(2,0)$	$2X^3+2X$	$2X+2$	$(2,2)$	2	$(0,2)$
8	$(2,1)$	$2X^3+X^2+2X+1$	$2X$	$(2,0)$	$X+1$	$(1,1)$
9	$(2,2)$	$2X^3+2X^2+2X+2$	$2X+1$	$(2,1)$	$2X$	$(2,0)$

Table 2
Behavior of $\mathcal{A}$

State	First component	Second component	Reached state
$(2,0)$	$(2,2)=\Phi(C_9)$	$(2,0)+\Phi(D_{9,1})=(1,0)$	$\Phi(D_{9,0})=(2,1)$
$(2,1)$	$(0,1)=\Phi(C_2)$	$(2,1)+\Phi(D_{2,1})=(0,0)$	$\Phi(D_{2,0})=(0,1)$
$(0,1)$	$(0,1)=\Phi(C_2)$	$(0,1)+\Phi(D_{2,1})=(1,0)$	$\Phi(D_{2,0})=(0,1)$
$(0,1)$	$(0,0)=\Phi(C_1)$	$(0,1)+\Phi(D_{1,1})=(0,1)$	$\Phi(D_{1,0})=(0,0)$

Instead of describing $\mathcal{A}$ which contains 9 states and 81 edges, we shall just check that the word

$$\begin{pmatrix}(0,1)(2,1)(2,2)(0,1)(0,1)(0,0)\\(1,2)(1,2)(1,0)(0,0)(1,0)(0,1)\end{pmatrix}=\begin{pmatrix}(0,0)\rho_B(P)\\\rho_B(P.Q)\end{pmatrix}^R$$

is accepted by $\mathcal{A}$ (u^R denotes the reversal of a word u). Starting from the initial state $(0,0)$ and reading $(0,1)=\Phi(C_2)$ on the first (upper) component, we must have $(0,0)+\Phi(D_{2,1})=(1,2)$ on the second (lower) component and go to state $(0,0)+\Phi(D_{2,0})=(0,1)$. From state $(0,1)$ and reading $(2,1)=\Phi(C_8)$, we must have on the second component $(0,1)+\Phi(D_{8,1})=(0,1)+(1,1)=(1,2)$ and go to the state $\Phi(D_{8,0})=(2,0)$. Continuing this way, we can summarize the behavior of $\mathcal{A}$ in Table 2.

Since $(0,0)$ is the unique final state of $\mathcal{A}$, this shows that the proposed word is accepted by $\mathcal{A}$.

Corollary 4. *Let γ be a nonzero element in $\mathbb{F}$ and $\mu:\{0,\dots,q-1\}\to\mathbb{F}$ be a one-to-one map such that $\mu(0)=0$. Let $\mu':\{0,\dots,q-1\}\to\mathbb{F}$ be such that $\mu'(j)=\gamma\mu(j)$, for all $j<q$. Then a set $\mathcal{T}\subseteq\mathbb{N}$ is (q,μ,B)-recognizable if and only if it is (q,μ',B)-recognizable.*

Proof. It is a special case of the previous proposition with $Q=\gamma$. □

4. Automaticity

This section results from some fruitful discussions with F. von Haeseler. Let S be a finite set and $f:\mathbb{F}[X]\to S$ be a mapping. Such a map is a natural generalization of the concept of infinite word usually indexed by $\mathbb{N}$ or $\mathbb{Z}$. We shall therefore use notation like $f=(f(P))_{P\in\mathbb{F}[X]}$. In particular, if $S=\{0,1\}$, each map f defines a partition of $\mathbb{F}[X]$ into two parts, namely $f^{-1}\{0\}$ and $f^{-1}\{1\}$. So a subset $\mathcal{T}$ of $\mathbb{F}[X]$ can be defined by its characteristic map $f_{\mathcal{T}}:\mathbb{F}[X]\to\{0,1\}$ which maps P onto 1 if and only if P belongs to $\mathcal{T}$.

Definition 4. Let S be a finite set. A map $f:\mathbb{F}[X]\to S$ is *B-recognizable* or *B-automatic* if for all $s\in S$, $f^{-1}\{s\}$ is a B-recognizable subset of $\mathbb{F}[X]$.

Remark 4. The terminology B-automatic can be explained as follows [4]. Let $S=\{s_1,\dots,s_k\}$. If $f:\mathbb{F}[X]\to S$ is *B-recognizable* then for all $s_i\in S$, $i=1,\dots,k$, there exists a (complete) deterministic finite automaton $\mathcal{A}_i=(Q_i,q_{0,i},\mathbb{F}^b,\delta_i,F_i)$ accepting $\mathbf{0}^*\rho_B(f^{-1}\{i\})$. As usual, one can consider the product automaton having $Q=Q_1\times\cdots\times Q_k$ as set of states, $q_0=(q_{0,1},\dots,q_{0,k})$ as initial state and where the transition function $\Delta:Q\times(\mathbb{F}^b)^*\to Q$ is defined by

$$\Delta\big((q_1,\dots,q_k),w\big)=\big(\delta_1(q_1,w),\dots,\delta_k(q_k,w)\big).$$

To this automaton, we associate an output function $\tau : Q \to S$ which maps $(q_1, \ldots, q_k)$ onto s_i if and only if $q_i \in F_i$. This function is well defined since f is a mapping, in $(q_1, \ldots, q_k)$ exactly one of the q_i's belongs to a set F_i. So the map f can be computed with this product automaton fed with B-representations of polynomials,

$$f(P) = \tau\big[\Delta\big(q_0, \mathbf{0}^n \rho_B(P)\big)\big], \quad \forall P \in \mathbb{F}[X],\ n \geqslant 0.$$

It is merely an exercise in automata theory to consider an automaton fed with reversal of B-representations ending with an arbitrary number of zeroes and computing the same map.

Definition 5. Let B be a polynomial of degree $b > 0$. For each $R \in \mathbb{F}[X]_{<b}$, we define a *B-decimation map*, $\partial_{B,R} : S^{\mathbb{F}[X]} \to S^{\mathbb{F}[X]}$ which maps $(f(P))_{P\in\mathbb{F}[X]}$ onto $(f(B.P + R))_{P\in\mathbb{F}[X]}$. The *$B$-kernel* of $f = (f(P))_{P\in\mathbb{F}[X]}$ is the set of all the maps obtained by applying an arbitrary number of decimation mappings to f,

$$\ker_B(f) = \big\{\partial_{B,R_1} \circ \cdots \circ \partial_{B,R_n}(f) \;\big|\; \forall n \geqslant 0,\ R_1, \ldots, R_n \in \mathbb{F}[X]_{<b}\big\}.$$

The following proposition is useful to prove the B-recognizability of some sets of polynomial.

Proposition 5. *A map $f : \mathbb{F}[X] \to S$ is B-recognizable if and only if its B-kernel is finite.*

Proof. The proof follows the same lines as in [4, Chapter 6]. □

An application of this proposition will be given in Remark 6.

5. Base dependence

For the usual k-ary numeration system, a set $\mathcal{T} \subseteq \mathbb{N}$ is said to be k-recognizable if the language made of the k-ary representations of the elements in X is regular. Let $k, \ell \geqslant 2$ be two multiplicatively independent integers, i.e., the only integer solution to $k^m = \ell^n$ is $m = n = 0$. The celebrated Cobham's theorem [6] states that if $\mathcal{T} \subset \mathbb{N}$ is simultaneously k-recognizable and ℓ-recognizable, then it is a finite union of arithmetic progressions. Otherwise stated, the characteristic map $f_{\mathcal{T}} : \mathbb{N} \to \{0, 1\}$ is *ultimately periodic*, i.e., $\exists N \geqslant 0,\ \exists p > 0,\ \forall i \geqslant N$: $f_{\mathcal{T}}(i) = f_{\mathcal{T}}(i + p)$. Consequently, the k-recognizability of a set depends strongly on the choice of the base k. In this section, we introduce this topic of the base dependence for the B-recognizability of sets of polynomials.

Proposition 6. *Let B be a polynomial of degree $b > 0$. A set $\mathcal{T} \subseteq \mathbb{F}[X]$ is B-recognizable if and only if it is B^k-recognizable, $k \in \mathbb{N} \setminus \{0\}$.*

Proof. Let P be a polynomial having the following two decompositions:

$$P = C_0\big(B^k\big)^\ell + C_1\big(B^k\big)^{\ell-1} + \cdots + C_{\ell-1}B^k + C_\ell$$

and

$$P = C_{0,k-1}B^{k\ell+k-1} + \cdots + C_{0,0}B^{k\ell} + \cdots + C_{\ell,k-1}B^{k-1} + \cdots + C_{\ell,0},$$

where $C_0 \neq 0$ and at least one of the $C_{0,i} \neq 0$, $\deg(C_i) < kb$ and $\deg(C_{i,j}) < b$. It is clear that we have the following relations:

$$C_i = C_{i,k-1}B^{k-1} + \cdots + C_{i,0}, \quad \forall i \in \{0, \ldots, \ell\}. \tag{3}$$

Since $\deg(C_i) \leqslant kb-1$, the polynomial coefficients $C_{i,j}$ appearing in those relations can be computed by $k-1$ successive Euclidian divisions and are thus completely determined by C_i and B. With our notation, $\Phi_{B^k}(P) = C_0 \ldots C_\ell \in (\mathbb{F}^{kb})^*$ and $\Phi_B(P) = C_{0,k-1} \ldots C_{0,0} \ldots C_{\ell,k-1} \ldots C_{\ell,0} \in (\mathbb{F}^b)^*$. We have a one-to-one correspondence between $\mathbb{F}^{kb}$ (respectively $\mathbb{F}^b$) and the set $\mathbb{F}[X]_{<kb}$ (respectively $\mathbb{F}[X]_{<b}$) of polynomials over $\mathbb{F}$ of degree less than kb (respectively less than b). Therefore to each symbol C_i of $\mathbb{F}^{kb}$ (which is a kb-tuple of elements in $\mathbb{F}$) we associate a word $C_{i,k-1} \cdots C_{i,0}$ of length k over $\mathbb{F}^b$ such that the relation (3) is satisfied. We have thus defined a k-uniform morphism $\tau_k : \mathbb{F}^{bk} \to (\mathbb{F}^b)^*$ (a morphism is *k-uniform* if the image of each letter is a word of constant length k) such that for all $u \in (\mathbb{F}^{bk})^*$,

$$\pi_{B^k}(u) = \pi_B\big(\tau_k(u)\big).$$

Notice that if u is the B^k-representation of a polynomial P, then $\tau_k(u)$ is the B-representation of the same polynomial (except that the latter representation could possibly begins with leading **0**'s). The conclusion follows from the fact that the set of regular languages is closed under morphism and inverse morphism. □

Example 6. Let $B = X^2 + 2X + 2$ be a polynomial over $\mathbb{F} = \mathbb{Z}/3\mathbb{Z}$. The morphism τ_2 that replaces a B^2-representation with a B-representation is given by

$$\begin{array}{lll}
(0,0,0,0) \mapsto (0,0)(0,0) & (0,0,0,1) \mapsto (0,0)(0,1) & (0,0,0,2) \mapsto (0,0)(0,2) \\
(0,0,1,0) \mapsto (0,0)(1,0) & (0,0,1,1) \mapsto (0,0)(1,1) & (0,0,1,2) \mapsto (0,0)(1,2) \\
\vdots & \vdots & \vdots \\
(0,2,2,0) \mapsto (0,2)(1,2) & (0,2,2,1) \mapsto (0,2)(1,0) & (0,2,2,2) \mapsto (0,2)(1,1) \\
(1,0,0,0) \mapsto (1,1)(2,1) & (1,0,0,1) \mapsto (1,1)(2,2) & (1,0,0,2) \mapsto (1,1)(2,0) \\
(1,0,1,0) \mapsto (1,1)(0,1) & (1,0,1,1) \mapsto (1,1)(0,2) & (1,0,1,2) \mapsto (1,1)(0,0) \\
\vdots & \vdots & \vdots \\
(1,2,2,0) \mapsto (1,0)(0,0) & (1,2,2,1) \mapsto (1,0)(0,1) & (1,2,2,2) \mapsto (1,0)(0,2) \\
(2,0,0,0) \mapsto (2,2)(1,2) & (2,0,0,1) \mapsto (2,2)(1,0) & (2,0,0,2) \mapsto (2,2)(1,1) \\
(2,0,1,0) \mapsto (2,2)(2,2) & (2,0,1,1) \mapsto (2,2)(2,0) & (2,0,1,2) \mapsto (2,2)(2,1) \\
\vdots & \vdots & \vdots \\
(2,2,2,0) \mapsto (2,1)(2,1) & (2,2,2,1) \mapsto (2,1)(2,2) & (2,2,2,2) \mapsto (2,1)(2,0)
\end{array}$$

For instance, the relation $2X^3 + 2X^2 + 2X + 2 = (2X+1)(X^2 + 2X + 2) + 2X$ gives the image by τ_2 of $(2,2,2,2)$ which is $(2,1)(2,0)$.

We can also consider the case of two "multiplicatively dependent" polynomials.

Corollary 7. *Let P and Q be two polynomials of degree at least one having the property that there exist two integers $k, \ell > 0$ such that $P^k = Q^\ell$. A set $\mathcal{T} \subseteq \mathbb{F}[X]$ is P-recognizable if and only if it is Q-recognizable.*

Proof. Thanks to the previous result, a set of polynomials is P-recognizable iff it is P^k-recognizable iff it is Q^ℓ-recognizable iff it is Q-recognizable. □

Example 7. Let $P = X^4 + X^3 + 2X^2 + 2X + 1$ and $Q = X^6 + 2X^3 + 2$ be two polynomials over $\mathbb{F} = \mathbb{Z}/3\mathbb{Z}$. The P-recognizable and Q-recognizable sets are the same since, over $\mathbb{F}$, $P^3 = Q^2 = (X^2 + 2X + 2)^6$.

As shown by the next proposition, multiplying the base B by a constant γ belonging to the field $\mathbb{F}$ does not affect the recognizability.

Proposition 8. *Let $\gamma \in \mathbb{F} \setminus \{0\}$. A set $\mathcal{T} \subset \mathbb{F}[X]$ is B-recognizable if and only if it is (γB)-recognizable.*

Proof. Consider the two decompositions of a same polynomial P with respect to the bases B and γB,

$$P = \sum_{i=0}^{k} C_i B^{k-i} = \sum_{i=0}^{k} \left(\gamma^{-1}\right)^{k-i} C_i (\gamma B)^{k-i}.$$

Set $\delta = \gamma^{-1}$. Clearly, $\deg(C_i) = \deg(\delta^{k-i} C_i)$. Let ℓ be the order of δ in $\mathbb{F}$. Consider the circular automaton $\mathcal{A}$ having $\{q_0, \ldots, q_{\ell-1}\}$ as set of states, $\mathbb{F}^b \times \mathbb{F}^b$ as alphabet, q_0 as initial state, where all states are final and where the transition function ξ is defined for any $C \in \mathbb{F}^b$ and $i \in \{0, \ldots, \ell - 2\}$ by

$$\xi\left(q_i, \begin{pmatrix} C \\ \delta^i C \end{pmatrix}\right) = q_{i+1}$$

and for any $C \in \mathbb{F}^b$ by

$$\xi\left(q_{\ell-1} \begin{pmatrix} C \\ \delta^{\ell-1} C \end{pmatrix}\right) = q_0.$$

This automaton accepts the reversal of the language composed by pairs of words of the form $(\rho_B(u), \rho_{\gamma B}(u))$, $u \in \mathbb{F}[X]$. Since B and γB have the same degree, the two components are words of the same length. □

Example 8. Let $\mathbb{F} = \mathbb{Z}/5\mathbb{Z}$ and $B = 3X^2 + 2X + 1$. Take

$$P = \sum_{i=0}^{4} (X + 1) B^i, \qquad \rho_B(P) = (1, 1)(1, 1)(1, 1)(1, 1)(1, 1).$$

Using notation of the previous proof, we consider $\gamma = 3$ and thus $\delta = \gamma^{-1} = 2$. Within $\mathbb{F}$, $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 3$ and $2^4 = 1$ ($\ell = 4$). An easy computation shows that

$$\rho_{3B}(P) = (1, 1)(3, 3)(4, 4)(2, 2)(1, 1).$$

Remark 5. One can also notice that if e is the order of $\gamma \in \mathbb{F}$ then $(\gamma B)^e = B^e$ and Proposition 8 can be considered as a corollary of Proposition 6. Nevertheless, the proof of Proposition 8 gives interesting information on the automata involved in this special case.

In the framework of integer bases, it is well known that arithmetic progressions are recognizable for any base. Here is an analogous result within the polynomial ring $\mathbb{F}[X]$.

Proposition 9. *Let M, Q, B be polynomials over $\mathbb{F}$ with* $\deg(B) \geqslant 1$. *The set*

$$\mathcal{A} = \left\{ P.M + Q \;\middle|\; P \in \mathbb{F}[X] \right\} \tag{4}$$

is B-recognizable.

Proof. This is a direct consequence of Proposition 3 and Corollary 2. □

Corollary 10. *Let $D \in \mathbb{F}[X]$ be a nonzero polynomial of degree d. The map r_D: $\mathbb{F}[X] \to \mathbb{F}[X]_{<d}$ mapping any polynomial P onto its remainder* mod D *is B-recognizable for any B.*

One can think about Cobham's theorem discussing base dependence properties for integer bases number systems [6]. Thanks to a discussion with D. Berend we have examples of sets recognizable in any base and not included in the previous proposition.

Remark 6. Consider the set $\mathcal{O}$ of polynomials of odd degree over a finite field $\mathbb{F}$,

$$\mathcal{O} = \left\{ P \in \mathbb{F}[X] \setminus \{0\} \;\middle|\; \deg(P) \equiv 1 \pmod 2 \right\}.$$

Let B be a polynomial of degree $b > 1$. Consider the characteristic map $f_{\mathcal{O}}$. We show that $\ker_B(f_{\mathcal{O}})$ contains at most two elements and therefore $\mathcal{O}$ is B-recognizable for any B. Clearly, if b is even, then for all nonzero polynomial $P \in \mathcal{O}$ (respectively $P \notin \mathcal{O}$) and all $R \in \mathbb{F}[X]_{<b}$, $B.P + R \in \mathcal{O}$ (respectively $B.P + R \notin \mathcal{O}$) so $\partial_{B,R}(f_{\mathcal{O}}) = f_{\mathcal{O}}$. In the same way, if b is odd, $\partial_{B,R}(f_{\mathcal{O}}) = 1 - f_{\mathcal{O}}$ and $\partial_{B,R}(1 - f_{\mathcal{O}}) = f_{\mathcal{O}}$. This example can also be trivially extended to

$$\mathcal{B} = \left\{ P \in \mathbb{F}[X] \setminus \{0\} \;\middle|\; \deg(P) \equiv r \pmod s \right\} \tag{5}$$

for any $0 \leqslant r < s$.

Thanks to Proposition 9 and Remark 6, the following result is obvious. We suspect that the subsets of $\mathbb{F}[X]$ described in this corollary are the only ones recognizable in any polynomial base B but a complete proof is still out of reach.

Corollary 11. *Any finite Boolean combination of sets of polynomials over $\mathbb{F}$ of the kind* (4) *and* (5) *is recognizable in any base.*

In many proofs of Cobham's theorem (and its generalizations to nonstandard numeration systems), syndeticity plays a central role. Recall that an infinite set of integers $X = \{x_0 < x_1 < \cdots\}$ is *syndetic* (or, *with bounded gaps*) if there exists $C > 0$ such that $x_{n+1} - x_n \leqslant C$ for all $n \geqslant 0$.

Assuming that a set $\mathcal{T} \subset \mathbb{N}$ is recognizable for two multiplicatively independent bases, following G. Hansel's scheme [11] a first step to prove Cobham's theorem is to show that $\mathcal{T}$ is syndetic (see for instance [4, Chapter 6] and [15]).

Definition 6. The usual notion of syndeticity could possibly be translated as follows, an infinite set $\mathcal{T} \subseteq \mathbb{F}[X]$ is *degree-syndetic* if there exists $C > 0$ such that for all $n \geqslant 0$,

$$\mathcal{T} \cap \big\{ P \in \mathbb{F}[X] \;\big|\; \deg(P) \in [n, n + C) \big\} \neq \emptyset,$$

i.e., the set $\{\deg(P) \mid P \in \mathcal{T}\}$ is a syndetic set of $\mathbb{N}$.

Proposition 12. *Let $\mathcal{T} \subseteq \mathbb{F}[X]$ be an infinite set and $B \in \mathbb{F}[X]$ of degree $b > 0$. If $\mathcal{T}$ is B-recognizable, then it is degree-syndetic.*

Proof. The language $\rho_B(\mathcal{T})$ is regular. It is well known that the set of lengths of a regular language is ultimately periodic (in the sense given at the beginning of this section). Otherwise stated, there exist $L, C > 0$ such that for all $\ell > L$, there exists a word of length $t \in [\ell, \ell + C)$ in $\rho_B(\mathcal{T})$. This means that $\mathcal{T}$ is degree-syndetic. □

Example 9. The set $\{X^{2^n} \mid n \geqslant 0\}$ is never B-recognizable.

The following example involves the celebrated Thue–Morse sequence and exhibit a set of polynomials recognizable in two independent bases.

Example 10. Let $\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$. Take

$$\mathcal{T} = \big\{ P \in \mathbb{F}[X] \;\big|\; P(1) = 0 \big\}.$$

Notice that $P(1) = 0$ if and only if P contains an even number of monomials. Since the celebrated Thue–Morse sequence is 2-automatic [4], the set of integers with binary expansion having an even number of 1's is 2-recognizable and with notation of Example 2, it is $(2, \mu, X)$-recognizable. So $\mathcal{T}$ is X-recognizable. On the other hand, it is clear that $\mathcal{T} = \{(X + 1).Q \mid Q \in \mathbb{F}[X]\}$, so $\mathcal{T}$ is also $(1 + X)$-recognizable. But, as a consequence of Proposition 9, this set is recognizable for all polynomial bases.

This latter example is in fact a special case of the following result.

Proposition 13. *Let $\beta, \gamma \in \mathbb{F}$ and $B \in \mathbb{F}[X]$ of degree $b > 0$. The set*

$$\mathcal{T} = \big\{ P \in \mathbb{F}[X] \;\big|\; P(\beta) = \gamma \big\}$$

is B-recognizable.

Proof. Indeed, for any polynomial P, we have

$$P(\beta) = \gamma \quad \Leftrightarrow \quad (P - \gamma)(\beta) = 0 \quad \Leftrightarrow \quad \exists Q \in \mathbb{F}[X]\colon\ (P - \gamma)(X) = (X - \beta).Q(X).$$

Thus $\mathcal{T} = \{(X - \beta).Q + \gamma \mid Q \in \mathbb{F}[X]\}$ and this set is recognizable thanks to Proposition 9. □

5.1. Complexity function

We would like to be able to characterize sets of polynomials over $\mathbb{F}$ which are recognizable in any base, just like the ones given in Corollary 11. For k-ary numeration systems over $\mathbb{N}$, a well-known result of M. Morse and G.A. Hedlund (see for instance [4]) could possibly be restated as follows. A set $\mathcal{T} \subseteq \mathbb{N}$ is a finite union of arithmetic progressions (and is therefore recognizable in any base) if and only if the characteric word of $\mathcal{T}$ has a complexity function (which maps $n \geqslant 0$ onto the number of factors of length n) bounded by a constant. As shown below, a direct analogous of this result is not so obvious to obtain over $\mathbb{F}[X]$, the reason being that the structures of $\mathbb{N}$ and $\mathbb{F}[X]$ are quite different.

Definition 7. Let $f : \mathbb{F}[X] \to S$ be a map. For all $P \in \mathbb{F}[X]$ and $n \geqslant 0$, we define the map

$$\zeta_f(P, n) : \mathbb{F}[X]_{<n} \to S : R \mapsto f(P + R).$$

The *complexity function* of f is $\mathfrak{C}_f : \mathbb{N} \to \mathbb{N}$ defined by

$$\mathfrak{C}_f(n) = \#\big\{\zeta_f(P, n) \;\big|\; P \in \mathbb{F}[X]\big\}.$$

It is clear that $\mathfrak{C}_f(n) \leqslant \mathfrak{C}_f(n+1) \leqslant (\mathfrak{C}_f(n))^q$ since $\zeta_f(P, n) \neq \zeta_f(Q, n)$ implies $\zeta_f(P, n+1) \neq \zeta_f(Q, n+1)$. Moreover, we have

$$1 \leqslant \mathfrak{C}_f(n) \leqslant (\#S)^{q^n}.$$

Let us fix any total ordering of $\mathbb{F}[X] = \{0 = R_1 < R_2 < \cdots\}$ such that

$$R_i \leqslant R_j \quad \Rightarrow \quad \deg(R_i) \leqslant \deg(R_j).$$

Therefore the complexity function of f maps n onto the number of distincts words

$$f(P + R_1), f(P + R_2), \ldots, f(P + R_{q^n}).$$

The following proposition shows that sets of the kind (5) do not have a complexity bounded by constant.

Proposition 14. *Consider the same notation as in* (4) *and* (5)*. If $\mathcal{A}$ and $\mathcal{B}$ satisfies respectively* (4) *and* (5)*, then for n large enough,*

$$\mathfrak{C}_{f_\mathcal{A}}(n) \leqslant q^{\deg(M)} \quad \textit{and} \quad \mathfrak{C}_{f_\mathcal{B}}(n) \geqslant n - r.$$

Proof. Assume that $\mathbb{F}[X] = \{R_1 < R_2 < \cdots\}$ has been ordered by increasing degree. The sequence $(f_\mathcal{A}(S + R_i))_{i \geqslant 0}$ depends only on S mod M which can takes $q^{\deg(M)}$ distinct values.

Now consider sets of the second kind. For all $P \in \mathbb{F}[X]$ and $i \leqslant q^n$, if $\deg(P) \geqslant n$, $f_\mathcal{B}(P + R_i)$ depends only on the degree of P mod s. This gives only two possibilities for such a P: for all $i \leqslant q^n$, $f_\mathcal{B}(P + R_i) = 0$ (respectively $f_\mathcal{B}(P + R_i) = 1$).

Any P such that $\deg(P) < r$ gives a single function, $f_\mathcal{B}(P + R_i) = 1$ for $i \in \{1, \ldots, q^n\}$ if and only if $\deg(R_i) \equiv r \bmod s$.

Finally consider any two polynomials P, Q such that $r \leqslant \deg(P) < \deg(Q) < n$, there exists R_i ($i \leqslant q^n$) such that $f_{\mathcal{B}}(P+R_i) \neq f_{\mathcal{B}}(Q+R_i)$. Indeed, one has to take a convenient polynomial R_i such that $\deg(R_i) = \deg(P)$ to force $\deg(P+R_i)$ to any value $d < \deg(P)$. If $P = a_g X^g + \cdots + a_{d+1}X^{d+1} + a_d X^d + \cdots + a_0$, just take $R_i = (-a_g)X^g + \cdots + (-a_{d+1})X^{d+1} + b_d X^d$ such that $a_d + b_d \neq 0$. Moreover, since $\deg(R_i) < \deg(Q)$, then $\deg(Q+R_i) = \deg(Q)$. If $\deg(Q) \equiv r \bmod s$ (respectively $\deg(Q) \not\equiv r \bmod s$) then choose $d \not\equiv r \bmod s$ (respectively $d \equiv r \bmod s$). This give at least $n-r$ different mappings (one for each of the considered degrees). □

6. Sequential operations

This short section is independent of the rest of the paper and consider only "automatic" computation. Notice that the fact that division by a fixed polynomial is sequential is explicitly mentioned as an example in [14]. As a consequence of this section, we estimate the complexity in terms of operations to compute the B-representation of a polynomial.

Definition 8. A *transducer* is a machine computing (generally, in a nondeterministic way) output words from input words [13]. More specifically, consider a nondeterministic finite automaton $\mathcal{A} = (Q, \Sigma^* \times \Delta^*, I, F, \delta)$ where Q is the finite set of states, I (respectively F) is the set of initial (respectively final) states and $\delta \subseteq Q \times \Sigma^* \times \Delta^* \times Q$ is the finite transition relation. A *successful path* in $\mathcal{A}$ is a sequence of consecutive edges belonging to δ, $(p_0, x_1, y_1, p_1)\cdots(p_{n-1}, x_n, y_n, p_n)$, where $p_0 \in I$, $p_n \in F$, the word $x_1 \ldots x_n \in \Sigma^*$ (respectively $y_1 \ldots y_n \in \Delta^*$) being the corresponding *input* (respectively *output*). The set of labels of all successful paths is a subset R of $\Sigma^* \times \Delta^*$: the *relation computed* by $\mathcal{A}$.

A transducer over $\Sigma \times \Delta^*$ is *pure sequential* if it has a unique initial state and the *underlying input automaton* is deterministic (this latter condition means that by taking the projection of δ on $Q \times \Sigma \times Q$, the resulting automaton is deterministic). In this case, for each word $x \in \Sigma^*$, there exists at most one $y \in \Delta^*$ such that $(x, y) \in R$. The transducer computes therefore a partial function $f : \Sigma^* \to \Delta^*$ which is said to be (*left*) *pure sequential*. A function $f : \Sigma^* \to \Delta^*$ is *right pure sequential* if the function $g : \Sigma^* \to \Delta^*$ defined by $f(x^R) = (g(x))^R$ is left sequential.

Finally, a (*left*) *sequential transducer* is a pair $(\mathcal{A}, \kappa)$, where $\mathcal{A}$ is defined as above and where $\kappa : Q \to \Delta^*$ maps each state onto an output word. If (x, y) is the label of a successful path in $\mathcal{A}$ ending in a state q, then the output produced by $(\mathcal{A}, \kappa)$ and corresponding to x is $y\kappa(q)$. In other words, at the end of the computation, κ is used to append to the output a word depending on the reached state. Considering again reversal, one can define *right sequential transducer*.

A slight adaptation of Proposition 3 shows that the function

$$\psi : \left(\mathbb{F}^b\right)^* \to \left(\mathbb{F}^b\right)^* : u \mapsto \rho_B\left(Q.\pi_B(u)\right)$$

is right sequential for any given polynomial B. Using the same kind of arguments, one shows that this function is also left sequential.

Now consider the Euclidian division of $P = p_0 X^n + \cdots + p_n$ by $B = b_0 X^\ell + \cdots + b_\ell$ ($n \geqslant \ell$). The quotient of P by B can be viewed as a left pure sequential function using a transducer having $\mathbb{F}$ as input alphabet. We only sketch the construction. Read consecutively $p_0, \ldots, p_{\ell-1}$ (the reading of the first ℓ coefficients does not produce any output, or equivalently the output

is ε) and when reading p_ℓ, write the symbol $p_0.b_0^{-1} \in \mathbb{F}$ as first output and reach a state of the form

$$\big(p_1 - p_0.b_0^{-1}.b_1, \ldots, p_\ell - p_0.b_0^{-1}.b_\ell\big) \in \mathbb{F}^\ell.$$

Being in a state $(q_0, \ldots, q_{\ell-1})$ and reading $x \in \mathbb{F}$, write the output $q_0.b_0^{-1}$ and go to the state

$$\big(q_1 - q_0.b_0^{-1}.b_1, \ldots, q_{\ell-1} - q_0.b_0^{-1}.b_{\ell-1}, x - q_0.b_0^{-1}.b_\ell\big).$$

The set of states of the transducer is $\mathbb{F}^\ell$ plus some extra states used only when reading the initial prefix $p_0, \ldots, p_{\ell-1}$. After reading $p_0, \ldots, p_n$, the outputs correspond to the coefficients of the quotient of the division of P by B and the state eventually reached corresponds to the remainder of the division (which is a polynomial of degree less than ℓ and thus determined by at most ℓ coefficients in $\mathbb{F}$).

Example 11. Let $P = 2X^4 + X^3 + 2X + 1$ and $B = X^2 + 2X + 2$ ($b_0 = 1$, $b_1 = b_2 = 2$) be two polynomials over $\mathbb{F} = \mathbb{Z}/3\mathbb{Z}$. We first read $p_0 = 2$ and $p_1 = 1$. Next we read $p_2 = 0$, write $p_0.b_0^{-1} = \mathbf{2}$ and go to the state $(p_1 - p_0.b_0^{-1}.b_1,\ p_2 - p_0.b_0^{-1}.b_2) = (0, 2)$. We now read $p_3 = 2$, write $0.b_0^{-1} = \mathbf{0}$ and go to the state $(2 - 0.b_0^{-1}.b_1, 2 - 0.b_0^{-1}.b_2) = (2, 2)$. From this state, we read $p_4 = 1$, write $2.b_0^{-1} = \mathbf{2}$ and go to the state $(2 - 2.b_0^{-1}.b_1, 1 - 2.b_0^{-1}.b_2) = (1, 0) = \Phi_X(X)$. In other words, this means that the quotient of P by B is $2X^2 + 2$ and the remainder is X.

Remark 7. We can use this transducer to compute the B-representation of a polynomial P. Using Remark 1, a first application of the transducer to the coefficients of P gives the remainder of the division of P by B and thus the last letter of $\rho_B(P)$. We now use the same transducer but this time fed not with P but with the output obtained at the first stage. We iterate this process. If $\deg(B) = b$ and $\deg(P) = k.b + r$, $r < b$, then the number of steps (one symbol read and/or written) needed to compute completely $\rho_B(P)$ is

$$k.b + r + (k-1).b + r + \cdots + b + r = \frac{k(k+1)}{2}b + k.r \in \mathcal{O}\big(b.k^2\big).$$

Acknowledgments

The author would like to thank Peter Grabner who suggested this work and also Friedrich von Haeseler and Daniel Berend for fruitful discussions. I also thanks the anonymous referees who evaluated an earlier version of this work submitted for DLT'05 (Development in Languages Theory, Palermo).

References

[1] J.-P. Allouche, Automatic sequences, in: Lectures Notes CANT'2006, Combinatorics, Automata and Number Theory, in: EMS MathSchools Ser. 2, Univ. of Liège, 2006.

[2] J.-P. Allouche, E. Cateland, W.-J. Gilbert, H.-O. Peitgen, J. Shallit, G. Skordev, Automatic maps in exotic numeration systems, Theory Comput. Syst. 30 (1997) 285–331.

[3] J.-P. Allouche, F. von Haeseler, H.-O. Peitgen, G. Skordev, Linear cellular automata, finite automata and Pascal's triangle, Discrete Appl. Math. 66 (1996) 1–22.

[4] J.-P. Allouche, J. Shallit, Automatic Sequences, Theory, Applications, Generalizations, Cambridge Univ. Press, Cambridge, 2003.
[5] V. Bruyère, G. Hansel, C. Michaux, R. Villemaire, Logic and p-recognizable sets of integers, Bull. Belg. Math. Soc. Simon Stevin 1 (1994) 191–238.
[6] A. Cobham, On the base-dependence of sets of numbers recognizable by finite automata, Math. Systems Theory 3 (1969) 186–192.
[7] M. Drmota, G. Gutenbrunner, The joint distribution of Q-additive functions on polynomials over finite fields, J. Théor. Nombres Bordeaux 17 (2005) 125–150.
[8] G.W. Effinger, D.R. Hayes, Additive Number Theory of Polynomials over a Finite Field, Oxford Univ. Press, New York, 1991.
[9] S. Eilenberg, Automata, Languages, and Machines, vol. A, Pure Appl. Math., vol. 58, Academic Press, New York, 1974.
[10] A. Fraenkel, Systems of numeration, Amer. Math. Monthly 92 (1985) 105–114.
[11] G. Hansel, À propos d'un théorème de Cobham, in: D. Perrin (Ed.), Actes de la fête des mots, Greco de programmation, CNRS, Rouen, 1982, pp. 55–59.
[12] M. Hbaib, M. Mkaouar, Sur le bêta-développement de 1 dans le corps des séries formelles, Int. J. Number Theory 2 (2006) 365–378.
[13] M. Lothaire, Algebraic Combinatorics on Words, Encyclopedia Math. Appl., vol. 90, Cambridge Univ. Press, Cambridge, 2002.
[14] C. Reutenauer, Subsequential functions: Characterizations, minimization, examples, in: Aspects and Prospects of Theoretical Computer Science, Smolenice, 1990, in: Lecture Notes in Comput. Sci., vol. 464, Springer, Berlin, 1990, pp. 62–79.
[15] M. Rigo, L. Waxweiler, A note on syndeticity, recognizable sets and Cobham's theorem, Bull. Eur. Assoc. Theor. Comput. Sci. EATCS 88 (2006) 169–173.
[16] K. Scheicher, β-expansions in algebraic function fields over finite fields, Finite Fields Appl. 13 (2007) 394–410.
[17] K. Scheicher, J. Thuswaldner, Digit systems in polynomial rings over finite fields, Finite Fields Appl. 9 (2003) 322–333.
[18] N.J.A. Sloane, The on-line encyclopedia of integer sequences, AT&T Knowledge Ventures, 2006, http://www.research.att.com/~njas/sequences/index.html.
[19] S. Wolfram, A New Kind of Science, Wolfram Media, Champaign, IL, 2002, http://www.wolframscience.com/nksonline/toc.html.